REMARKS

The Examiner has rejected Claims 32-47 under 35 U.S.C. 103(a) as being unpatentable over Herbert, U.S. Patent No.: 5,333,183, in view of Bowman, U.S. Patent No.: 5,627,886. Applicant respectfully disagrees with such rejection.

In the previous response to Office Action filed January 5, 2004, applicant emphasized that the Herbert reference fails to disclose, teach or suggest any sort of gatherer state monitoring let alone "utilizing the state of the gatherers and the stored data records to recover from the fault upon the detection thereof" (emphasis added). In response, the Examiner now further relies on the Abstract; col. 2, line 1 – col. 3, line 40; and col. 11, lines 28-53 of Bowman, in combination with Herbert, in order to make a prior art showing.

After careful review of such excerpts from Bowman, however, it is clear that Bowman simply discusses, in the background section thereof, techniques for detecting fraudulent network usage. Moreover, in reviewing the remaining Bowman reference, the only mention of state is in the context of a "Fraud state database 154." However, similar to Herbert, there is simply no discussion of gatherer state monitoring, let alone "utilizing the state of the gatherers and the stored data records to recover from the fault upon the detection thereof" (emphasis added).

Only applicant teaches and claim such a specific filtering and aggregating gatherer state-based recovery in combination with the remaining features for allowing a more thorough recovery from a fault in the specific aggregation/filtering framework, as currently claimed.

To establish a *prima facie* case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be

found in the prior art and not based on applicant's disclosure. *In re Vaeck*,947 F.2d 488, 20 USPQ2d 1438 (Fed.Cir.1991).

Applicant thus respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met, since the Examiner's cited excerpts do not disclose, teach or suggest applicant's claim language, as set forth hereinabove.

In the previous response, applicant further amended each of the independent claims to require "filtering and aggregating the network communications usage information utilizing a plurality of gatherers, wherein the filtering and aggregating are based on a user-defined configuration," (emphasis added). In response, the Examiner has relied upon the abstract; col. 2, line 27 – col. 3, line 4; and col. 7, lines 30-59 of Bowman (see below) to make a prior art showing of the foregoing added claim limitations.

"In the accomplishment of these and other objects, a computerized system and method for detecting fraudulent network usage patterns using real-time network monitoring of at least two disparate networks is shown which receives at least one event record from each of the disparate networks, analyzes each of the received event records to determine its type based on user-defined parameters, identifies predetermined fields in the analyzed event record to be used as keys, measures network usage associated with the key, summarizes usage statistics against at least one of the keys, compares statistic totals to predefined thresholds, and responds with an alarm or the like when the thresholds are met or exceeded.

The Fraud Management System (FMS) of the present invention effectively detects usage patterns indicative of many types of known fraud including: calling card related fraud, cellular phone fraud, subscription fraud, hacking, call selling, 900/800 fraud, and PBX or CPE fraud, among others. As a result, the FMS provides a means for detecting and ultimately preventing fraudulent use of communications or credit card/business networks. Monitoring network usage for fraudulent telecommunications network usage patterns according to the present invention takes place outside the switch and normally after the call event has completed.

The system monitors network usage on an event-by-event basis, accepting event record detail information from multiple network sources. As fraud is dynamic, exploiting new technologies and services nearly as quickly as they are deployed, the system also possesses a high degree of configurability. Fraud system administrators are able to create new detection mechanisms without the need to write new programs. Finally, the system and method of the present invention supports an analysis of trends in network usage, so that "early warnings" of new types of fraud are available.

The system and method of the present invention assists in detecting fraudulent use of a communications network by monitoring the network to detect usage patterns typically indicative of fraud. The present system is not limited to detecting the types of fraud known to exist today. It is a general-purpose system that can be configured to detect many different sorts of usage patterns. Thus, as new types of fraud arise, they can be detected without time-consuming and costly coding changes; instead the system's configuration data can be changed to respond to these new threats as they arise." (col. 2, line 27 - col. 3, line 4)

"Simulator 180 is used to test the system configuration before it is released into production. Before any new profile or algorithm is released, Simulator 180 can be used to test the accuracy of new changes to the system. Simulator 180 may also be used to test the system in the absence of live records from SCPs 50 or pricing system 75. Simulator 180 can use manually entered call events or call events recorded by the system in production.

Returning now to FIG. 2, as noted above, the fraud monitoring system of the present invention

> supports interfaces to a variety of sources of call detail data: standard wireline, wireline information services, analog cellular, digital cellular, analog roaming cellular, etc. Separate inbound interfaces 110 are preferably developed for each source for increased speed of input. Each interface, in turn, has three components: data collector 100, inbound interface 110 and event logger 122. The general capabilities among data collectors 100, among inbound interfaces 110, and among event loggers 122 are identical. They differ only in the event record formats they handle and in the communication protocols used with their respective network elements.
>
> Specifically, data collector 100 is a computer directly connected to the call detail data source or network. It reads incoming raw call detail records (CDRs), filters out CDRs irrelevant to fraud detection, reformats relevant CDRs into standardized FMS internal formats, passes UNIX files of standardized CDRs to its respective inbound interface 110, logs throughput statistics to UNIX flat files and permits manual reconfiguration through a graphical interface so one data collector can provide backup for another when necessary." (col. 7, lines 30-59)

Such excerpts, however, merely suggest generally the analysis of event records to determine their type, based on user-defined parameters. Thus, the mere mention of a user-defined record type-analysis does not rise to the level of specificity of applicant's claimed user-defined filtering and aggregating.

Moreover, such excerpts suggest a "reformatting" of CDR's, which falls short of applicant's claimed "aggregating." Thus, the mere mention of a "manual configuration" of the data collector does not rise to the level of specificity of applicant's claimed user-defined filtering and aggregating.

Again, applicant thus respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met, since the Examiner's cited excerpts do not disclose, teach or suggest applicant's claim language, as set forth hereinabove.

Applicant further notes that the Examiner's rejection is further deficient with respect to the dependent claims and Claim 47. A notice of allowance or a specific prior art showing of each of the claim limitations, in combination with the remaining claim elements, is respectfully requested.

Moreover, the Examiner has not addressed applicant's previous arguments. For example, the Examiner continues to argue that Claim 47 is substantially the same as Claims 32-36, and is thus rejected for the reasons set forth for those in the rejection of Claims 32-36. This is simply incorrect. Applicant emphasizes that there are numerous additional features in Claim 47 that distinguish the Herbert and Bowman combination, and have not been fully considered by the Examiner. For example, see the following limitations:

"defining a user-defined enhancement procedure utilizing the central event manager," and "enhancing the aggregation with the gatherers in accordance with the defined enhancement procedure;"

"normalizing the network communications usage information with the gatherers by excluding fields not required by a central event manager coupled to the gatherers;" and

"time stamping the data records; storing the time stamped data records in tables in a central database coupled to the central event manager at a user-specified interval; deleting the stored data records upon the cessation of a predetermined amount of time after the storage utilizing the timestamp."

A specific prior art showing of the foregoing limitations or an indication of allowable subject matter is respectfully requested.

In the event a telephone conversation would expedite the prosecution of this application, the Examiner may reach the undersigned at (408) 505-5100. For payment of the fees due in connection with the filing of this paper, the Commissioner is authorized to charge such fees to Deposit Account No. 50-1351 (Order No. XACTP014C).

Respectfully submitted,

Kevin J. Zilka
Registration No. 41,429

P.O. Box 721120
San Jose, CA 95172-1120
408-505-5100